de: 5001-06

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID: DoD-2022-OS-0081]

Privacy Act of 1974; System of Records

AGENCY: DoD Office of Inspector General (DoD OIG), Department of Defense (DoD).

ACTION: Notice of a new system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the DoD is establishing a new system of records titled, "OIG Data Analytics Platform, CIG-30." This system of records covers the DoD OIG collection and maintenance of records necessary in order to fulfill the responsibilities of the Inspector General Act of 1978, as amended. The DoD OIG will use this system of records to develop data models and analytical assessments that will assist with the performance of audits, evaluations, investigations, and reviews in order to identify fraud, waste, and abuse relating to the programs and operations of the DoD. Additionally, DoD is issuing a Notice of Proposed Rulemaking, which proposes to exempt this system of records from certain provisions of the Privacy Act, elsewhere in today's issue of the *Federal Register*.

DATES: This system of records is effective upon publication; however, comments on the Routine Uses will be accepted on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. The Routine Uses are effective at the close of the comment period.

ADDRESSES: You may submit comments, identified by docket number and title, by either of the following methods:

* Federal Rulemaking Portal: https://www.regulations.gov. Follow the instructions for submitting comments.

* Mail: Department of Defense, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Regulatory Directorate, 4800 Mark Center Drive, Attn:

Mailbox 24, Suite 08D09, Alexandria, VA 22350-1700.

Instructions: All submissions received must include the agency name and docket number for this *Federal Register* document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at https://www.regulations.gov as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Anna Rivera, DoD OIG, FOIA, Privacy and Civil Liberties Office, 4800 Mark Center Drive, Alexandria, VA 22350; email: privacy@dodig.mil, (703) 699-5680.

SUPPLEMENTARY INFORMATION:

I. Background

The DoD OIG is establishing the OIG Data Analytics Platform, CIG-30 as a Privacy Act system of records. The DoD OIG Data Analytics Team (DAT) will use this system of records to develop data models and analyses in order to identify fraud, waste and abuse, and programmatic problems and deficiencies. This system of records will allow the DoD OIG DAT to identify correlations between existing DoD data sets and other government agency data sets so as to identify patterns and correlations that indicate fraud and issues of program waste and abuse. This system of records will also be used to identify problems or failures in the implementation or performance of internal controls within the DoD by using existing datasets within DoD databases and applying analytics and data modeling principles to identify deficiencies, anomalies, and trends that may identify fraud, waste, and abuse. Additionally, DoD is issuing a Notice of Proposed Rulemaking, which proposes to exempt this system of records from certain provisions of the Privacy Act, elsewhere in today's issue of the *Federal Register*.

DoD system of records notices (SORNs) have been published in the *Federal Register* and are available from the address in FOR FURTHER INFORMATION CONTACT or at the Office

of the Assistant to the Secretary of Defense for Privacy, Civil Liberties and Transparency (OATSD(PCLT) website at https://dpcld.defense.gov/.

II. Privacy Act

Under the Privacy Act, a "system of records" is a group of records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined as a U.S. citizen or lawful permanent resident.

In accordance with 5 U.S.C. 552a(r) and Office of Management and Budget (OMB) Circular No. A-108, OATSD(PCLT) has provided a report of this system of records to the OMB and to Congress.

Dated: July 14, 2022.

Aaron T. Siegel,

Alternate OSD Federal Register

Liaison Officer, Department of Defense.

SYSTEM NAME AND NUMBER: OIG Data Analytics Platform, CIG-30.

SECURITY CLASSIFICATION: Unclassified, Classified.

SYSTEM LOCATION: Department of Defense (Department or DoD), located at 1000 Defense Pentagon, Washington, DC 20301-1000, and other Department installations, offices, or mission locations. Information may also be stored within a government-certified cloud, implemented and overseen by the Department's Chief Information Officer, 6000 Defense Pentagon, Washington, DC 20301-6000.

SYSTEM MANAGER: DoD Office of Inspector General (OIG), Data Analytics Team (DAT), Technical Director, 4800 Mark Center Drive, Alexandria, VA 22350-1500.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 10 U.S.C. 141, Inspector General; Inspector General Reform Act of 2008 (Pub. Law 110-409); Inspector General Empowerment Act of 2016 (Pub. Law 110-317); Executive Order 9397 (SSN), as amended; and DoD Directive 5106.01, Inspector General of the Department of Defense.

PURPOSE(S) OF THE SYSTEM:

A. To carry out the DoD OIG's responsibilities of conducting and overseeing audits, evaluations, investigations, and reviews relating to DoD programs and operations pursuant to the Inspector General Act of 1978, as amended.

B. To identify internal control weaknesses and to provide information required for conducting and overseeing audits, evaluations, investigations, and reviews relating to DoD programs and operations.

C. To promote economy, efficiency, and effectiveness in the administration of such programs and operations.

D. To prevent and detect fraud, waste, and abuse by performing data modeling and conducting data analysis to detect fraud, waste, and abuse in DoD programs and operations.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: All Military Services personnel, including from National Guard and Reserve components; former members and

retirees of the Military Services; dependent family members of Military Services members; DoD "affiliated" individuals (e.g., non-appropriated fund employees working on military installations, Red Cross volunteers assisting at military hospitals, United Services Organization (USO) staff providing services on military installations, Congressional staff members visiting military installations, etc.); DoD presidential appointees; and DoD civilian employees, contractor personnel, or individuals (and their surviving beneficiaries) accorded benefits, rights, privileges, or immunities associated with DoD as provided by U.S. law.

CATEGORIES OF RECORDS IN THE SYSTEM: The OIG Data Analytics Platform, CIG-30, system of records will contain a wide variety of records to carry out its purpose across the DoD. The following categories of records may be collected from existing DoD information systems and/or the information systems of other agencies to the extent that information is pertinent to a DoD OIG audit, evaluation, investigation, or review:

A. Personal and employment information such as: individual's full name, DoD Identification Number, Social Security Number (SSN), date of birth, marital status, race, gender, duty positions, payment histories, home addresses, physical addresses, driver's license numbers and telephone numbers.

B. Medical information such as: dates of treatment, medical/dental diagnosis, prescription drug information, location of care, pharmacy records, immunization records, Medical and Physical Evaluation Board records, laboratory test results, dental records, family medical history, death records, medical insurance records, and health risk assessments.

C. Financial information, including: bank account numbers and transactions, contracting and business ownership data, and Electronic Funds Transfer Numbers.

D. Cybersecurity information, including: Internet Protocol (IP) addresses, email addresses, and electronic signature data such as media access control (MAC) addresses, International Mobile Equipment Identity (IMEI) numbers, Router or network signatures, Public Key Infrastructure keys and credit card metadata.

RECORD SOURCE CATEGORIES: Records and information stored in this system of records are obtained from publicly available sources and various systems of records and information systems within the DoD and other Federal, State, local and foreign government agencies.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, all or a portion of the records or information contained herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the federal government when necessary to accomplish an agency function related to this system of records.

B. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

C. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.

D. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

E. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

F. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

G. To appropriate agencies, entities, and persons when (1) the DoD suspects or confirms a breach of the system of records; (2) the DoD determines as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD OIG's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

H. To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

I. To another Federal, State or local agency for the purpose of comparing to the agency's system of records or to non-Federal records, in coordination with an Office of Inspector General in conducting an audit, investigation, inspection, evaluation, or some other review as authorized by the Inspector General Act.

J. To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

K. To the news media and the public with the approval of the DoD Inspector General in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DoD, or when disclosure is necessary to demonstrate the accountability of DoD's officers, employees, or

individuals covered by the system, except to the extent the Inspector General determines that release of the specific information in the context of a particular case would constitute a clearly unwarranted invasion of personal privacy.

L. To designated officers, contractors, and employees of Federal, State, local, territorial, tribal, international, or foreign agencies for the purpose of the hiring or retention of an individual, the conduct of a suitability or security investigation, the letting of a contract, or the issuance of a license, grant or other benefit, to the extent that the information is relevant and necessary to the agency's decision on the matter and that the employer is appropriately informed about information that relates to or may impact an individual's suitability or eligibility.

M. To other Federal Inspector General offices, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), or other law enforcement agencies for the purpose of coordinating and conducting audits, reviews, administrative inquiries, civil or criminal investigations, or when responding to such offices in connection with the investigation of a potential violation of law, rule, and/or regulation.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records will be stored electronically. The records may be stored on magnetic disc, tape, or digital media; in agency-owned cloud environments; or in vendor Cloud Service Offerings certified under the Federal Risk and Authorization Management Program (FedRAMP).

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by individual name, SSN, DoD ID number, or driver’s license number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records are retained and disposed of in accordance with the applicable records schedule for the systems from which they were collected. Any unscheduled records will be retained indefinitely, until they have been scheduled with the National Archives and Records Administration and have become eligible for disposition under those schedules.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: The DoD safeguards records in this system of records according to applicable rules, policies, and procedures, including all applicable DoD automated systems security and access policies. DoD policies require the use of controls to minimize the risk of compromise of personally identifiable information (PII) in paper and electronic form and to enforce access by those with a need to know and with appropriate clearances. Additionally, the DoD established security audit and accountability policies and procedures that support the safeguarding of PII and detection of potential PII incidents. The DoD routinely employs safeguards to information systems and paper recordkeeping systems, such as the following: Multifactor log-in authentication including Common Access Card (CAC) authentication and password; physical token as required; physical and technological access controls governing access to data; network encryption to protect data transmitted over the network; disk encryption securing disks storing data; key management services to safeguard encryption keys; masking of sensitive data as practicable; mandatory information assurance and privacy training for individuals who will have access; identification, marking, and safeguarding of PII; physical access safeguards including multifactor identification physical access controls, detection and electronic alert systems for access to servers and other network infrastructure; and electronic intrusion detection systems in DoD facilities.

RECORD ACCESS PROCEDURES: Individuals seeking access to their records should address written inquiries to the DoD OIG Freedom of Information Act, Privacy and Civil Liberties Office, 4800 Mark Center Drive, Alexandria, VA 22350-1500; www.dodig.mil/FOIA or foiarequests@dodig.mil. Signed written requests should contain the name and number of this system of records notice along with full name, current address, and email address of the individual and any details which may assist in locating records of the individual. In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the appropriate format:

If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)."

If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

CONTESTING RECORD PROCEDURES: The DoD rules for accessing records, contesting contents, and appealing initial agency determinations are contained in 32 CFR part 310, or may be obtained from the system manager.

NOTIFICATION PROCEDURES: Individuals seeking to determine whether information about themselves is contained in this system of records should follow the instructions for Record Access Procedures above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: DoD has exempted records maintained in this system from 5 U.S.C. 552a(c)(3), (c)(4), (d)(1)-(4), (e)(1), (e)(2), (e)(3), (e)(4)(G) through (I), (e)(5), (e)(8), (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2). The DoD also has exempted records maintained in this system from 5 U.S.C. 552a(c)(3), (d)(1)-(4), (e)(1), and (e)(4)(G) through (I), and (f) of the Privacy Act pursuant to 5 U.S.C. 552a(k)(1) and (k)(2). An exemption rule for this record system has been promulgated in accordance with the requirements of 5 U.S.C. 553(b)(1), (2), and (3), (c) and (e) and published in 32 CFR 310. In addition, when exempt records received from other systems of records become part of this system, DoD also claims the same exemptions for those records that are claimed for the prior system(s) of records from which they were a part and claims any additional exemptions set forth here.

HISTORY: None.

[FR Doc. 2022-15457 Filed: 7/19/2022 8:45 am; Publication Date: 7/20/2022]